EMIL FORD
Lawyers

Keyboard punches: a school's duty of care in the domain of cyberbullying

Sarah Heydon – October 2018

TABLE OF CONTENTS

ABOUT THE AUTHOR

Sarah Heydon is a lawyer at Emil Ford Lawyers. She practises mainly in education law, adoptions, and wills and estate planning. Sarah assists in advising educational institutions throughout Australia.

Sarah is a member of the NSW Chapter of the Australia and New Zealand Education Law Association and a regular contributor to *Education Law Notes*, which keep schools throughout Australia up-to-date with education law developments. She is also a member of the NSW Committee on Adoption and Permanent Care. Sarah has presented to school and charity administrators on governance issues.

Sarah Heydon BA LLB (Hons)

Emil Ford Lawyers

Level 5, 580 George Street

SYDNEY NSW 2000

T 02 9267 9800

F 02 9283 2553

E Sarah.Heydon@emilford.com.au

Keyboard punches: a school's duty of care in the domain of cyberbullying

Sarah Heydon
Emil Ford Lawyers

What is this paper about?

Bullying is no longer confined to the school premises before the final bell of the day rings. Since the Internet is everywhere, we have entered a new frontier where bullying has the potential to happen anywhere at any time. This takes the form of cyberbullying.

It is estimated that one in seven children of school age in Australia are being cyberbullied.[1] Considering that in 2017 there were 3,849,225 students enrolled in Australian schools,[2] this produces the sobering statistic that 549,889 students in Australia are being cyberbullied. As such, the majority of our schools have no doubt had a student harass or humiliate another student via social media or other online avenues.

This paper begins by examining what cyberbullying is, how a school's liability arises and what consequences a school may face. The paper then turns to consider the liability of Internet Service Providers (ISPs), the cyberbully's parents and the cyberbully themselves. The paper concludes by examining what steps schools should take to prevent and respond to cyberbullying.

To give some international context, I consider the situation in the United Kingdom, Canada and the United States throughout the paper.

[1] Alannah & Madeline Foundation, *eSmart Schools: FAQs* (February 2018) 2, <https://www.amf.org.au/media/2425/esmart-schools-faqs.pdf>.
[2] Australian Bureau of Statistics, *4221.0 – Schools, Australia, 2017* (2 February 2018) <http://www.abs.gov.au/ausstats/abs@.nsf/mf/4221.0>.

Identifying when cyberbullying is occurring

To identify cyberbullying and to understand the legal liability for it, one must first define what it is. Bullying, more generally, has been defined as "**repeated intimidation**, **over time**, of a **physical**, **verbal** or **psychological** (including indirect and relational bullying) nature of a less powerful person by a more powerful person or group of persons."[3]

Cyberbullying, more specifically, is defined by the Office of the eSafety Commissioner as "the use of **technology** to **bully** a person or group with the **intent to hurt** them **socially**, **psychologically** or even **physically**."[4]

Legislative backing for this definition is found in the *Enhancing Online Safety Act 2015* (Cth). This Act establishes the eSafety Commissioner, sets out the Commissioner's functions and powers, provides for a complaints system for cyberbullying material and outlines the Commissioner's enforcement mechanisms. It provides a comprehensive definition of "cyber-bullying material targeted at an Australian child". Although schools are not bound by this legislative definition, it is nevertheless instructive for school leaders and teachers. Section 5 of the Act reads as follows:

(1) For the purposes of this Act, if material satisfies the following conditions:

> *(a) the material is provided on a* ***social media service*** *or* ***relevant electronic service****;*
>
> *(b) an* ***ordinary reasonable person*** *would conclude that:*
>
> > *(i) it is* ***likely*** *that the material was* ***intended*** *to have an* ***effect*** *on a particular Australian child; and*
> >
> > *(ii) the material would be* ***likely*** *to have the* ***effect*** *on the Australian child of* ***seriously threatening***, ***seriously***

[3] This definition was used by Professor Phillip Slee and David Ford almost 20 years ago: PT Slee and DC Ford, "Bullying is a Serious Issue – It is a Crime!" (1999) 4(1) *Australia & New Zealand Journal of Law & Education* 23, 28.
[4] Office of the eSafety Commissioner, *Cyberbullying* Australian Government <https://www.esafety.gov.au/esafety-information/esafety-issues/cyberbullying>.

> ***intimidating**, **seriously harassing** or **seriously humiliating** the Australian child;*
>
> *(c) such other conditions (if any) as are set out in the legislative rules;*
>
> *then:*
>
> *(d) the material is cyber-bullying material targeted at the Australian child; and*
>
> *(e) the Australian child is the target of the material.*
>
> *(2) An effect mentioned in subsection (1) may be:*
>
> *(a) a direct result of the material being **accessed by**, or **delivered to**, **the Australian child**; or*
>
> *(b) an indirect result of the material being **accessed by**, or **delivered to**, **one or more other persons**. [my emphasis]*

It follows that the first element of cyberbullying, and what distinguishes it from bullying more generally, is the use of **technology**. This includes social media services,[5] such as Facebook, Instagram, Twitter and Snapchat. It also includes other electronic services, such as email, instant messaging, text messaging, multimedia messaging (images and videos), online chat services and even online gaming services that enable players to interact or communicate with each other.[6]

The second element of cyberbullying is that of **threatening**, **intimidating**, **harassing** or **humiliating** a child **socially**, **psychologically**, **verbally** or even **physically**. However, not all incidents of such behaviour are bullying. The Act defines "cyber-bullying material" narrowly. The material, whether written, an image, a video or the like, must be more than merely offensive or insulting.[7] It must satisfy thresholds relating to objective reasonableness, intent and seriousness. In other words, it must be such that a **reasonable person** would conclude that, firstly, it is likely that the material was

[5] *Enhancing Online Safety Act 2015* (Cth) s 4.
[6] Ibid.
[7] Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 (Cth) 10.

intended to have an effect on a particular child and, secondly, the material would be likely to have a **serious** effect.

The third element is that the material must be **accessed by**, or **delivered to**, the particular child or one or more other persons (for example, their peers). This is unlike the definition of bullying generally, which usually requires that there are a number of individual incidents that take place over time. Collectively, those incidents comprise bullying behaviour. However, the Act does not **explicitly** require that the intimidating material be repeatedly accessed or delivered over time in order to constitute "cyber-bullying material".

Of course, if repetition over time is absent, that is, it is a one-off nasty email or text message, it will likely be harder to satisfy the objective reasonableness, intent and seriousness thresholds. So it could be said that the Act **implicitly** requires repetition over time of the intimidating material to constitute "cyber-bullying material".

However, it also recognises that the means, or technology, by which cyberbullying is conducted can have **inbuilt repetition over time**. Take Facebook for example. If John posts a nasty status update, image or video about Sam, all of John's friends can see the post. If John tags Sam in the post, all of Sam's friends can also see the post. Furthermore, if John's friend, Kate, and Sam's friend, Amy, react, comment or share the post, Kate's friends and Amy's friends may see the post. If John, Sam, Kate and Amy each have 500 friends, the post has the potential to be seen by thousands of people almost immediately, but it could also keep appearing on their newsfeeds for a number of days.

Understanding the liability of the school

Duty of care

Schools may be liable for the damage suffered by a student due to being bullied. This includes cyberbullying. The liability arises because schools and teachers owe a duty of care to all their students. In turn, the duty of care arises when a teacher-student relationship exists.

It is very clear that the requisite relationship exists, and the school has a duty of care for its students, while they are at school during usual school hours.[8] Mason J, as he was then, articulated this duty in the High Court of Australia: "A school authority owes to its pupils a duty to ensure that reasonable care is taken of them whilst they are on school premises during hours when the school is open for attendance."[9] Indeed, in *Cox v State of New South Wales*,[10] there was no question that the school owed a duty of care to the student because he was bullied on school premises during school hours. Therefore, when students are at school, the school owes them a duty of care.

What is the scope of the duty?

However, the duty does not cease upon the ringing of the final bell of the day or stop at the school gate. The school's duty of care exists beyond the school premises and before and after school hours.

In *Geyer v Downs*,[11] an eight-year-old student was injured in the school playground at about 8:50 am – 10 minutes before playground supervision started and 35 minutes before classes commenced. She was accidentally struck on the head by a softball bat held by another student whom she was

[8] This paper concentrates on the common law duty of care but schools ought not forget the very onerous statutory duty placed on them by their state's workplace, health and safety legislation.
[9] *The Commonwealth of Australia v Introvigne* (1982) 150 CLR 258, 269.
[10] [2007] NSWSC 471 ('*Cox*').
[11] (1977) 138 CLR 91 ('*Geyer*').

walking behind on her way to her classroom. As a result, she suffered very severe injuries. The High Court of Australia made the following observations about the "temporal ambit"[12] of the school's duty of care:

> *… The reference to "school hours" is not to be understood as more than a quite general reference to periods when, for the purpose of his education, a child is placed beyond "the control and protection of his parent".*[13]
>
> *There is no case which lays down that there is no duty of supervision prior to "school hours", however that expression may be understood… There seems no basis for treating it as a rule that there can be no duty of supervision outside "ordinary school hours" or "before school started". The question must depend upon the nature of the general duty to take reasonable care in all the circumstances.*[14]

In this case, the headmaster had arranged for the school grounds to be opened prior to 9:00 am to permit the entry of school students. He did that with the knowledge of the risks of injury involved from children playing ball games in a small and crowded playground without supervision. The only step taken to prevent that injury was an instruction given to the students that they were not to play or run around. Consequently, the Court held that the school's duty of care extended outside school hours:

> *When the plaintiff was injured there was already owed to her that morning a duty of care on the part of the headmaster, the relationship of schoolmaster and pupil having already come into existence. The headmaster had permitted her to come onto the school premises and had there subjected her to his control by*

[12] Ibid (Stephen J).
[13] Ibid.
[14] Ibid (Murphy and Aickin JJ).

> *requiring her, as an early-arriving pupil, to comply with the instructions he had laid down for such pupils.*[15]

In *Trustees of the Roman Catholic Church for the Diocese of Bathurst v Koffman*,[16] the student had left the school for the day and had walked 300 to 400 metres down the road to a bus stop outside another school where he intended to catch a bus. The student was injured when a student from the other school threw a stick and injured his eye.

The Supreme Court of New South Wales found that the school's duty of care extended outside school hours and away from school grounds. In reaching this conclusion, one of the judges, Mahoney P, said that a school owes a duty of care to the student when a school accepts a student and the school accepts a student when it assumes obligations towards the student such as to take appropriate care for the student's safety.[17] Therefore, Mahoney P felt that it was a question of determining what the school's obligations were in the circumstances rather than determining whether or not the school had any obligations. Sheller JA agreed, saying:

> *… I do not think the relationship of teacher and pupil begins each day when the pupil enters the school ground and terminates when the pupil leaves the school ground. Undoubtedly however a particular duty of care arises because of the pre-existing relationship.*[18]
>
> *In my opinion the extent and nature of the duty of the teacher to the pupil is dictated by the particular circumstances. I do not think its extent is necessarily measured or limited by the circumstance that*

[15] Ibid (Stephen J).
[16] (1996) Aust Torts Reports 81-399; BC9603487 1 ('*Koffman*').
[17] Ibid 6.
[18] Ibid 10.

> *the final bell for the day has rung and the pupil has walked out the school gate.*[19]

Sheller JA went so far as to say that if the school knew that students were bullied while travelling on the bus or while walking to or from school, the duty could extend to require the school to take preventative measures.[20]

What does this mean for cyberbullying?

There have not been any cases decided in Australia specifically about the scope of a school's duty of care when it comes to cyberbullying of its students. The same factors of whether the student is cyberbullied on or around school premises and whether the cyberbullying occurs during or around school hours are relevant but not determinative. There are other factors to consider; for example, whether or not the cyberbullying occurs via a school-hosted website and school computers are used.

Having examined the scope of a school's duty of care generally, the following hypotheses can be made about how far it might extend in terms of geography and time to include cyberbullying:

- based on *Cox*, there is no doubt that the scope of a school's duty of care will encompass cyberbullying via a **school-hosted website on school premises during school hours using school computers**.[21]
- based on *Geyer,* a duty of care may arise where students **use school computers on school premises**, **whether during school hours or**

[19] Ibid 11.
[20] Ibid 12-13.
[21] Marilyn Campbell, Des Butler and Sally Kift, 'A school's duty to provide a safe learning environment: Does this include cyberbullying?' (2008) 13 *Australia and New Zealand Journal of Law and Education* 21, 25; Desmond A Butler, 'Civil Liability for cyber bullying in schools: A new challenge for psychologists, schools and lawyers' in K Moore (ed), *Proceedings Psychology making an impact: the Australian Psychological Society 42nd Annual Conference* (Australian Psychological Society, 2007) 52, 54; Sally Kift, Marilyn Campbell and Des Butler, 'Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools' (2009-2010) 20 *Journal of Law, Information and Science* 60, 89; Des Butler, Sally Kift and Marilyn Campbell, 'Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?' (2009) 16 *eLaw Journal: Murdoch University Electronic Journal of Law* 84, 108-109.

not, to access **websites hosted on third party servers**, such as Facebook. This would of course depend on whether the school has control over the hosting server and whether it has granted remote access to students under conditions of use.[22]

- based on *Koffman,* the scope of a school's duty of care is also likely to catch cyberbullying via a **school-hosted website** which is accessed **away from school premises outside of school hours using personal computers**. Again, this will depend on the school's level of control over the hosting server and whether it has imposed conditions of use on remote access by students.[23]

However, if a bully uses their mobile phone while on school premises to send an intimidating text message, image or video to another student who is away from school premises (or vice versa, if the bully is away from school premises and the other student is on school premises), the existence of a duty of care is less clear.[24] It is possible in situations such as this, as well as those that might otherwise fall outside the ambit of a school's responsibility, that if the school has knowledge of cyberbullying taking place, as in *Koffman*, the requisite teacher-student relationship may be in existence.

Therefore, how far the scope of a school's duty of care extends when it comes to the cyberbullying of its students will depend on the facts and circumstances of each case. The following factors should be taken into account:

- whether the cyberbully and recipient are on or around school premises and/or,
- whether the cyberbullying occurs during or around school hours and/or,

[22] Campbell, Butler and Kift, above n 21, 25; Butler, above n 21, 54; Kift, Campbell and Butler, above n 21, 89-90; Butler, Kift and Campbell, above n 21, 109.
[23] Campbell, Butler and Kift, above n 21, 25; Butler, above n 21, 54; Kift, Campbell and Butler, above n 21, 89; Butler, Kift and Campbell, above n 21, 109.
[24] Butler, Kift and Campbell, above n 21, 109.

- whether it occurs via a school-hosted website and/or,
- whether school computers are used and/or,
- whether the school has knowledge of the cyberbullying taking place (especially if the other factors are not satisfied).

United Kingdom

This expansive interpretation of the scope of a school's duty of care contrasts with the restrictive interpretation in England. *Bradford-Smart v West Sussex County Council*[25] concerned a situation where the school knew of bullying taking place on the bus to and from school, although it was not taking place on school premises.[26] The Court of Appeal held that the school was not liable for the injury caused by the bullying outside of school, reasoning that a school does not owe a duty to its students to monitor their activities when they have left the school gates.[27] The Court reconciled that intervention by the school might have done more harm than good.[28]

United States

With the exception of Alaska,[29] every state has incorporated electronic ways of bullying into school bullying or harassment laws by amending their existing state statutory codes. Some state codes limit the scope of a school's duty of care to cyberbullying that occurs on school property or is carried out using school property, that is, via the school's Internet network or with school computers. For example, the Student Harassment Prevention Act, which is a chapter of the 2013 Code of Alabama, reads:

> *No student shall engage in or be subjected to harassment, intimidation, violence, or threats of violence* ***on school property, on***

[25] [2002] EWCA Civ 7.
[26] Ibid [32].
[27] Ibid.
[28] Ibid [35].
[29] Stop Bullying.gov, *Alaska Anti-Bullying Laws & Policies* (8 September 2017) U.S. Department of Health and Human Services <https://www.stopbullying.gov/laws/alaska/index.html>.

> ***a school bus, or at any school-sponsored function*** *by any other student in his or her school system. [my emphasis]*[30]

Similarly, the Elementary and Secondary Education chapter of the North Carolina General Statutes prohibits bullying and harassing behaviour, which is defined as:

> *… any pattern of gestures or written, electronic, or verbal communications, or any physical act or any threatening communication,* ***that takes place on school property, at any school-sponsored function, or on a school bus****… [my emphasis]*[31]

However, other state legislatures have embraced an expansive interpretation of the scope of a school's duty of care by explicitly incorporating off-campus cyberbullying into the ambit of a school's responsibility. For example, the Discipline subchapter of the 2012 Arkansas Code requires every school to adopt policies to prohibit bullying not only "while in school, on school equipment or property" and the like, but also "by an electronic act that results in the substantial disruption of the orderly operation of the school or educational environment."[32] Relevantly, this applies:

> *to an electronic act* ***whether or not the electronic act originated on school property or with school equipment****, if the electronic act is directed specifically at students or school personnel and maliciously intended for the purpose of disrupting school and has a high likelihood of succeeding in that purpose. [my emphasis]*[33]

However, the cyberbullying legislation has not received a great deal of attention from the courts. This is because cyberbullying cases are usually decided in the context of students' First Amendment rights. The First Amendment reads:

---

[30] AL Code § 16-28B-4(a) (2013).
[31] N.C. Gen. Stat. § 115C-407.15.
[32] AR Code § 6-18-514(e)(2)(B)(i)-(ii)(a) (2012).
[33] AR Code § 6-18-514(e)(2)(B)(b) (2012).

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*

As a result, courts have been very protective of students' free speech rights.[34] Indeed, they are bound to be. For example, the 2012 Arkansas Code states that nothing in the Discipline subchapter "is intended to… [u]nconstitutionally restrict protected rights of freedom of speech, freedom of religious exercise, or freedom of assembly."[35]

Consequently, schools face potential liability from victims when they do not act forcefully against cyberbullying and potential liability from off-campus bullies should courts find that schools have infringed their First Amendment rights.[36] As a result, schools tread a fine line between doing nothing and doing too much.[37] However, this lose-lose situation is fairly unique to the United States.

When will the school have breached their duty of care?

Returning to consider the Australian context, to determine whether a school has breached its duty of care, a court will consider whether the risk to the student was foreseeable, whether the risk was more than insignificant and

---

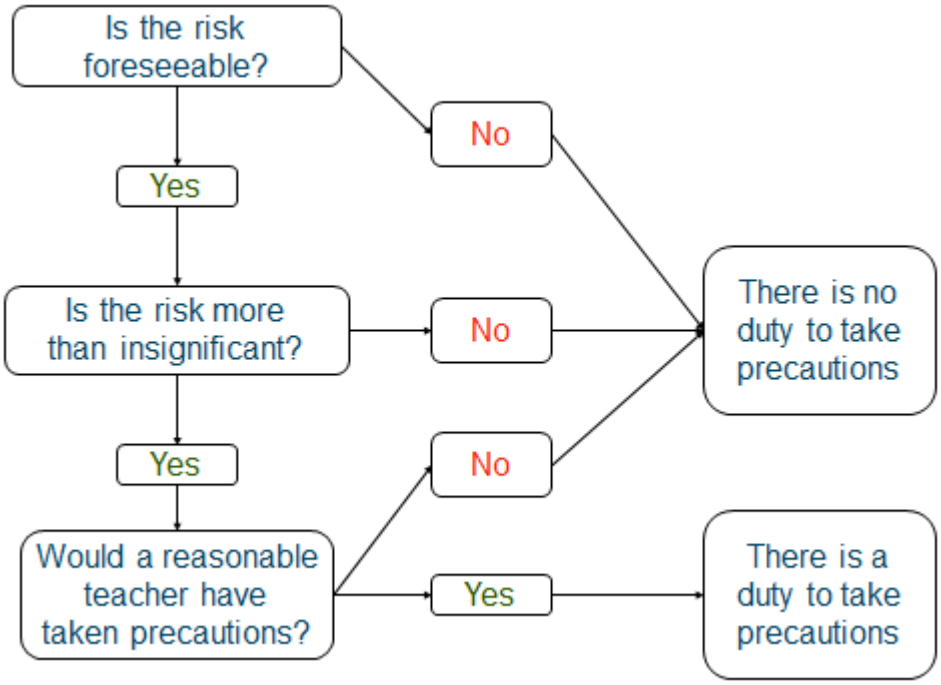
[34] Matthew Fenn, 'A Web of Liability: Does New Cyberbullying Legislation Put Public Schools in a Sticky Situation?' (2012) 81 *Fordham Law Review* 2729, 2752, 2756; Sonja Trainor, 'School Bullying Poses Legal Issues for School Boards' [2011] (August) *Leadership Insider* 1, 1; Todd D Erb, 'A Case for Strengthening School District Jurisdiction To Punish Off-Campus Incidents of Cyberbullying' (2008) 40 *Arizona State Law Journal* 257, 271; Darryn Cathryn Beckstrom, 'State Legislation Mandating School Cyberbullying Policies and the Potential Threat to Students' Free Speech Rights' (2008) 33 *Vermont Law Review* 283, 309-311; Séamus P Boyce and Andrew A Manna, 'School Liability for Bullying and Harassment' [2011] (August) *Leadership Insider* 1, 1-3; Jamison Barr and Emmy Lugus, 'Digital Threats on Campus: Examining the Duty of Colleges To Protect Their Social Networking Students' (2011) 33 *Western New England Law Review* 757, 771; Darcy K Lane, 'Taking the Lead on Cyberbullying: Why Schools Can and Should Protect Students Online' (2011) 96 *Iowa Law Review* 1791, 1794.

[35] AR Code § 6-18-514(j)(2) (2012).

[36] Fenn, above n 34, 2765; Karla Schultz, 'Free To Be Mean? What Are the First Amendment Rights of Bullies?' [2011] (August) *Leadership Insider* 3, 3.

[37] Fenn, above n 34, 2765; Schultz, above n 36, 4.

whether the school took all reasonable precautions to prevent the risk of harm to the student. If the risk was foreseeable and more than insignificant and the school or its staff did not take the precautions that the court believes a reasonable person would have taken in the circumstances, the school and its staff will be in breach of their duty of care. This process is illustrated in the following chart:



When we consider cyberbullying at a school, the risk is clearly foreseeable and more than insignificant. Therefore, the issue that must be considered is what reasonable precautions ought to be taken to minimise the risk of harm to students through bullying.

An example of where there was a failure to take reasonable precautions against the relevant risk was found in *Cox*.[38] Starting when Ben Cox was in kindergarten, an older boy repeatedly harassed and bullied Ben over about an 18-month period. Mrs Cox reported what was happening to teachers and Department officers. The teachers told Mrs Cox that they would keep an eye

[38] [2007] NSWSC 471.

on Ben and try to keep him away from the bully. They also told her that the bully had Attention Deficit Disorder and that this probably explained his behaviour. One of the Department officers told her that bullying builds character and that he thought it was a good thing that Ben got bullied.

Unsurprisingly, the Supreme Court of New South Wales found the teachers and the Department failed to take any reasonable steps to protect Ben from repeated harassment and bullying. Therefore, they had breached their duty of care to him. The Court said that:

> *… the conduct of [the bully] was expressly and repeatedly brought to the attention of various teachers, including at the highest level in the school. ... this was not an isolated incident, which occurred unexpectedly, and which the school could not reasonably be expected to have foreseen. This conduct was conduct which was not only foreseeable, but of which the school had actual and repeated notice. As a consequence, it was necessary that the school take greater than normal steps to eliminate the bullying in this case.*[39]
>
> *The suggestions that [the bully] suffered from Attention Deficit Disorder imply that the staff were well aware of his behavioural problems. ... [The bully's] propensities were known to the school authorities independently of anything brought to their attention by Mrs Cox; and even if that were not so, the school was thoroughly on notice after Mrs Cox's repeated complaints about the behaviour of [the bully] towards [Ben].*[40]

There was no evidence to suggest that the school had taken even basic reasonable precautions. The school had not taken any steps to implement effective anti-bullying programs, to educate staff and students, to have a management plan for eradicating bullying, or anything else. Basically, the

[39] Ibid [85].
[40] Ibid [81].

Court said "[t]he staff made no attempt to deal with a serious problem"[41] and "[t]he school authorities responded quite inadequately to an escalating problem and failed to take such steps as were reasonably required to protect [Ben] from the conduct of a plainly behaviourally disturbed older pupil."[42] I examine what steps schools should take to prevent and respond to cyberbullying later in this paper.

Compensation claims

To make a successful claim against a school, a student must establish four matters:

1. that the school owed the student a duty of care;
2. that the school breached its duty;
3. that the student suffered damage, injury or loss; and
4. that the damage was caused by the breach.

I have already considered the school's duty and when the school may breach its duty. I now turn to damage and causation.

Damages for negligence

It is uncontroversial that courts will award damages for physical injury. If a student is physically injured by a bully and the school had breached its duty of care, the school will be liable for the student's physical injury. However, in many bullying claims, and especially cyberbullying claims, the damage suffered by a student is not necessarily physical; a student may suffer a psychiatric illness.

To recover for damages for a psychiatric illness, the injured student must show that the breach by the school or teacher has caused psychiatric illness. The English Court of Appeal in *Bradford-Smart v West Sussex County Council* said:

[41] Ibid [93].
[42] Ibid [100].

> *We would add that in all these cases it is necessary to identify with some precision any breach of duty found. It is also important to consider whether the steps proposed would have been effective in preventing the bullying. It is not enough to find that there has been bullying, to find some breach of duty, and then to find that the bullying caused the injury.* ***There must be a causal connection between the breach of duty and the injury.*** *That will often be difficult to prove. [my emphasis]*[43]

In *Mount Isa Mines Ltd v Pusey*,[44] Windeyer J said:

> *It is, however, today a known medical fact that severe emotional distress can be the starting point of a lasting disorder of mind or body, some form of psychoneurosis or a psychosomatic illness. For that,* ***if it be the result of a tortious act,*** *damages may be had. [my emphasis]*[45]

Essentially, cyberbullied students, like bullied students more generally, must establish that, but for one or more of the school's or teacher's negligent acts or omissions, they would not be suffering their psychiatric condition. The school will often seek to point to other causes of the bullied student's condition. For example, the school could argue that the usual symptoms of cyberbullying can be indistinguishable from those simply associated with growing up,[46] which is entirely plausible.

Indeed, in *Cox*, the Department argued that the true cause of Ben's condition was to be found in either or both of his genetic history and the unintentionally malign influence of his mother who had a long history of depression and psychiatric difficulties.[47] However, the Court found that the bullying events were **a** cause of Ben's condition. In other words, the

[43] [2002] EWCA Civ 7, [37].
[44] (1970) 125 CLR 383.
[45] Ibid 394-395.
[46] Kift, Campbell and Butler, above n 21, 93; Butler, Kift and Campbell, above n 21, 111.
[47] [2007] NSWSC 471, [120].

negligence on the part of the teachers and the Department was found to be a necessary condition of the occurrence of the harm to Ben.

What liability is there to pay damages for mental harm?

The cyberbullied student, like the bullied student more generally, must suffer some harm for which the law will compensate. It is well settled that physical injury will be compensated. It is also clear that a bullied student can recover compensation for psychiatric illness which results from physical injury negligently inflicted by the defendant.[48] But will the law compensate for pure mental harm? This will depend on the jurisdiction. Most jurisdictions have passed legislation limiting or preventing compensation for pure mental harm. For example, in New South Wales, section 31 of the *Civil Liability Act* provides "[t]here is no liability to pay damages for pure mental harm resulting from negligence unless the harm consists of a recognised psychiatric illness."

In *Cox*, the Department sought to argue that Ben could only recover damages if he could prove that by virtue of some physical injury caused by the bullying he suffered from a recognisable psychiatric illness. On the basis of section 31, the Court had no difficulty in rejecting this argument and concluding that Ben was entitled to an award of damages because there was ample evidence that he suffered from a recognisable psychiatric illness.

Schools will be relieved to hear that, as Fenn puts it, "a line must be drawn somewhere – schools surely cannot regulate all of their students' activity, no matter what it is or where it takes place."[49] If the cyberbullying falls outside the ambit of a school's responsibility, it could be the concern of another defendant.

[48] *Jaensch v Coffey* (1984) 155 CLR 549, 565 (Brennan J).
[49] Fenn, above n 34, 2762.

Internet Service Provider and search engine liability

An ISP is a company that provides subscribers with access to the Internet. Examples of Australian ISPs include Telstra-Bigpond, Optus, TPG, iiNet, Dodo, iPrimus, Belong, Tomi, Bendigo Bank Telco, MyRepublic and Harbour ISP. Most schools and households subscribe to one of these ISPs. Once connected, subscribers use search engines, such as Google, to navigate the Internet.

There have not been any cases decided in Australia about ISP or search engine liability for the damage suffered by a user due to being cyberbullied. As such, I consider proceedings commenced against an ISP for cyberbullying in Canada, actions brought against ISPs for defamation in the United States and United Kingdom, and a claim brought against a search engine for defamation in Australia. I hypothesise what these actions mean for ISP and search engine liability for cyberbullying in Australia.

Canada

In the mid-2000s, the classmates of David Knight, an Ontario high schooler, set up an abusive website about him. The homepage had a photograph of David and read "Welcome to the page that makes fun of Dave Knight". The website falsely described him as a homosexual, a drug trafficker and a paedophile.[50] The website received millions of hits and many participants, on the invitation of the website's creators, contributed insults and derogatory comments about David and his family. Yahoo!, the website host, refused to take down the website for fear of breaching the classmates and participants' free expression rights. After six months, David brought a claim against Yahoo!, together with the school board (in relation to supervision). Before proceedings commenced, Yahoo! closed down the website. As a

[50] Shaheen Shariff and Dianne L Hoff, 'Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace' (2007) 1 *International Journal of Cyber Criminology* 76, 85; Carmen Pickering, 'The Jury Has Reached Its Verdict… Or Has It? Cyberbullying in the Canadian legal arena' (2008-2009) 89 *Alberta Teachers' Association Magazine* 1, 3-4.

result, judgement was not given and presumably David reached an out of court settlement with Yahoo!.

United States

In the United States, courts have been hesitant to subject ISPs to liability. This is because section 230 of the *Communications Decency Act* has been interpreted by courts as providing a "fairly broad shield" or "immunity" for ISPs with respect to communications initiated by others.[51] It reads:

> *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*

In *Zeran v America Online Inc.*,[52] the United States Court of Appeals, Fourth Circuit, held that the Act granted immunity to AOL. That is, AOL was not liable for the wrongs committed by its users. It should be noted that this was not a case about cyberbullying. The facts were that an unidentified third party, acting without Mr Zeran's knowledge or authority, posted a series of notices, which included Mr Zeran's name and telephone number, on AOL's electronic "bulletin board". The notices were advertising t-shirts and other items with slogans glorifying the April, 1995 bombing in Oklahoma City, in which 168 people were killed. Predictably, Mr Zeran received numerous disturbing and threatening telephone calls from people outraged with the posted notices. He claimed AOL was negligent in allowing the notices to remain and reappear on AOL's "bulletin board" (despite having received complaints from Mr Zeran following the appearance of the first advertisement), refusing to post retractions of those

[51] Jacqueline D Lipton, 'Cyberbullying and the First Amendment' (2012) 14 *Florida Coastal Law Review* 99, 113-114; Jacqueline D Lipton, 'Combating Cyber-Victimization' (2011) 26 *Berkeley Technology Law Journal* 1103, 1132; Robert G Magee and Tae Hee Lee, 'Information Conduits or Content Developers? Determining Whether News Portals Should Enjoy Blanket Immunity from Defamation Suits' (2007) 12 *Communication Law and Policy* 369, 370.
[52] 129 F 3d 327 (4th Cir, 1997).

notices and failing to screen for similar postings thereafter. The Court found in favour of AOL, saying:

> *Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred. The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication...*[53]

This decision was affirmed in *John Doe v GTE Corporation*.[54] The United States Court of Appeals, Seventh Circuit, held that the Act granted immunity to GTE Corporation.[55] However, Easterbrook J questioned the wisdom of *Zeran* and the merit of eliminating liability for ISPs.[56]

There are compelling policy reasons in favour of holding ISPs accountable. Notwithstanding their unwillingness to assist in unmasking online wrongdoers,[57] unlike schools or parents, ISPs are able to overcome the anonymity of cyberspace by identifying and locating a cyberbully.[58] They are also in a position to monitor and control damaging online conduct because they are generally able to track communications sent via their

[53] Ibid II.A.
[54] 347 F 3d 655 (7th Cir, 2003)
[55] Ibid; Shariff and Hoff, above n 50, 89-91.
[56] *John Doe v GTE Corporation*, 347 F 3d 655 (7th Cir, 2003); Shariff and Hoff, above n 50, 91.
[57] Lipton, above n 51, 114; Victoria Smith Ekstrand, 'Unmasking Jane and John Doe: Online Anonymity and the First Amendment' (2003) 8 *Communication Law and Policy* 405, 416; Lyrissa Barnett Lidsky, 'Anonymity in Cyberspace: What Can We Learn from John Doe?' (2009) 50 *British Columbia Law Review* 1373, 1374.
[58] Lipton, above n 51, 113.

services.[59] That said, it is unrealistic to expect ISPs to take sole responsibility for such communications.[60] It would be too costly and difficult in light of the sheer amount of information traffic being transmitted through ISPs.[61]

United Kingdom

Unlike the United States courts, the High Court of England and Wales has been willing to hold an ISP accountable for defamation. In *Godfrey v Demon Internet Ltd*,[62] the Court said that ISPs should be held liable under defamation legislation when they have knowledge of the offending material and either do not remove it within a reasonable amount of time or fail to act altogether.[63]

Australia

In a similar vein, the High Court of Australia has been willing to hold a search engine accountable for defamation. In *Trkulja v Google LLC*,[64] Mr Trkulja alleged that Google defamed him, when people searched for his name or alias, by displaying images that conveyed imputations that he was:

- "a hardened and serious criminal in Melbourne";
- in the same league as figures such as "convicted murderer" Carl Williams, "underworld killer" Andrew "Benji" Veniamin, "notorious murderer" Tony Mokbel and "Mafia Boss" Mario Rocco Condello;
- an associate of Veniamin, Williams and Mokbel; and

[59] Ibid.
[60] Ibid 113-114.
[61] Ibid 114; Pickering, above n 50, 3.
[62] [2001] QB 201.
[63] Ibid; Shariff and Hoff, above n 50, 109; Pickering, above n 50, 3.
[64] [2018] HCA 25.

- "such a significant figure in the Melbourne criminal underworld that events involving him are recorded on a website that chronicles crime in [the] Melbourne criminal underworld."[65]

Before commencing proceedings, Mr Trkulja wrote to Google, drawing the allegedly defamatory matter to their attention and making various demands to resolve the issue.[66] Google acceded to some of his demands but declined to remove the images of him that appeared in response to other image searches made using the search engine.[67] Mr Trkulja brought an action against Google on the basis of its "knowledge of the falsity of the imputations" and "its refusal to accept any responsibility for the allegedly defamatory publications".[68]

The trial judge held that Google did publish the images, the images were defamatory of Mr Trkulja and Google was not entitled to immunity from suit.[69] The High Court agreed.[70] Interestingly, the Court said:

> *… The liability of a search engine proprietor, like Google, may well turn more on whether the search engine proprietor is able to bring itself within the defence of innocent dissemination than on whether the content of what has been published has the capacity to defame.*[71]

In the context of cyberbullying, this means that it may not be difficult to prove that the published cyberbullying material is defamatory. As such, the search engine will likely be liable unless the defence of innocent dissemination applies.

The reason ISPs are not held accountable in the United States is because of strong freedom of speech protections. The situation in Australia is very

[65] Ibid [3]-[4].
[66] Ibid [15].
[67] Ibid [16].
[68] Ibid [17].
[69] Ibid [24].
[70] Ibid [35], [38], [61].
[71] Ibid [62].

different. Therefore, in accordance with the decision of the High Court of England and Wales, it is likely that Australian ISPs will be liable if they have knowledge of the cyberbullying material and do not respond reasonably or at all.

Parental liability

There is a question as to whether an action may be brought against the cyberbully's parents, particularly as they may be perceived as having the resources to meet a compensation claim.

Australian law begins with the presumption that a parent is not legally liable for the wrongdoing of their child.[72] However, there are circumstances in which this presumption may be rebutted. A parent may be liable for the consequence of their child's wrongdoing if:

1. they have in some way participated in, directed or ratified the wrongdoing of their child; or
2. it was occasioned or caused by their own negligence.[73]

Such negligence may arise from a parent failing to exercise reasonable control over the activities of their child or from a parent "arming" their child; that is, giving them "an instrument which it could reasonably be thought might be used by the child in a manner that would be dangerous to other persons."[74]

In *McHale v Watson*, Barry Watson, a 12-year-old child, threw a sharpened piece of metal, described as a dart, against a post, expecting it to stick. On hitting the post, the dart ricocheted off at an angle, striking Susan McHale, a nine-year-old child, in her right eye, resulting in permanent blindness in that eye. Windeyer J, for the High Court of Australia, held that, on the evidence,

[72] *Smith v Leurs* (1945) 70 CLR 256; *McHale v Watson* (1964) 111 CLR 384, 386-387 (Windeyer J).
[73] *McHale v Watson* (1964) 111 CLR 384, 386-387 (Windeyer J).
[74] Ibid.

Barry's father did not for some purpose give Barry a dart.[75] Therefore, his father was not negligent. His Honour went on to consider, if his view of the facts was wrong (that is, if Barry's father did give Barry a dart), whether he would have found Barry's father was indeed negligent. He said:

> *It is not negligent merely to allow a boy of twelve to have such a thing. Suppose he were allowed to have a pocket knife, a wooden sword, or even a toy bow and arrow. A parent does not incur responsibility for a misuse, not reasonably foreseeable, that a child makes of a thing that he could reasonably be expected to use safely. The case here is quite different from allowing a child, not old enough to be trusted with a firearm or not properly taught how to handle firearms, to have a gun. A gun is a thing that in its normal use must be handled with skill. I conclude therefore, that, on no version of the facts, could Watson senior be held guilty of negligence.*[76]

This case was decided in 1964 – well before cyberbullying, by virtue of the Internet, came into being. Reasoning by analogy, is giving a child a mobile phone or a computer with Internet access simply an object or toy that they are commonly allowed in today's society, much like a pocket knife, wooden sword or toy bow and arrow? Or is giving a child such a device more akin to a gun, something that must be handled with skill? Pickering conceives of a computer as a "dangerous machine".[77] However, it would be difficult to argue that the mere act by a parent of giving a child a mobile phone or a computer with Internet access amounts to "arming" a child.[78] It is unlikely that that a parent would be found to be negligent on this ground.

It is also unlikely that a parent would be found to be negligent on the ground of failing to exercise reasonable control over the activities of their child.

---

[75] Ibid.
[76] Ibid.
[77] Pickering, above n 50, 5.
[78] Butler, Kift and Campbell, above n 21, 98.

Even if a parent situates the computer with Internet access in a public place in the home, it is near impossible for even the most prudent parent to supervise their child at all times.[79] Nor is a parent "to know that a seemingly innocent message has a sinister connotation", couched in abbreviations, slang or code.[80] Therefore, it is doubtful that Australian courts would hold a parent liable for any damage suffered by another child due to being cyberbullied by their child.

Canada

Other common law jurisdictions have taken a different view. Between 2013 and 2015, Nova Scotia, Canada was one such jurisdiction. The legislature enacted the *Cyber-safety Act 2013*, which not only conceived of the scope of a school's duty of care narrowly, but held parents liable for any damage suffered by another child as a consequence of being cyberbullied by their child. Section 3 of the Act read:

(2) For the purpose of this Act, where a person who is a minor engages in an activity that is cyberbullying and a parent of the person

> *(a) knows of the activity;*
>
> *(b) knows or ought reasonably to expect the activity to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation; and*
>
> *(c) fails to take steps to prevent the activity from continuing,*

the parent engages in cyberbullying .

Section 22 of the Act reinforced the presumption of parental liability, but made provision for liability to be avoided by showing due diligence:

(3) Where the defendant is a minor, a parent of the defendant is jointly and severally liable for any damages awarded to the plaintiff unless the parent

[79] Ibid.
[80] Ibid; Kift, Campbell and Butler, above n 21, 82.

satisfies the Court that the parent was exercising reasonable supervision over the defendant at the time the defendant engaged in the activity that caused the loss or damage and made reasonable efforts to prevent or discourage the defendant from engaging in the kind of activity that resulted in the loss or damage.

However, in the 2015 case of *Crouch v Snell*,[81] the Supreme Court of Nova Scotia held that the Act infringed the *Canadian Charter of Rights and Freedoms*, which is part of the Constitution. Two former business partners had become entangled in Internet exchanges that amounted to cyberbullying under the Act. Mr Crouch sought a Protection Order pursuant to the Act. However, the Court held that the Order was a nullity because the Act on which it was based was unconstitutional. The Court found that it violated fundamental freedoms, such as "freedom of thought, belief, opinion and expression, including freedom of the press and other media communication" and it also violated the right to liberty.

In response, the Nova Scotia legislature enacted the *Intimate Images and Cyber-protection Act 2017*. Interestingly, all references to parental liability have been removed, as have all references to school liability. Therefore, in Nova Scotia there is no longer a legislative basis for holding parents liable for any damage suffered by another child as a result of being cyberbullied by their child.

United States

In the early 2000s, the Supreme Court of Pennsylvania showed some support for holding parents liable for negligent supervision of their child.[82] However, this has not been further developed by the courts.

---

[81] 2015 NSSC 340.

[82] In *J S v Bethlehem Area School District* 807 A 2d 847, 851 (Pa, 2002), J S, a year eight student, created a website on his own computer while at home. The website, titled "Teacher Sux", contained several web pages that made derogatory comments about his algebra teacher and the principal. It included a parody of his teacher as Hitler and encouraged other students to donate money to help hire a hitman to kill her. Both the teacher and the

Bully liability

A cyberbullied student may be able to pursue civil and criminal actions against the cyberbully. However, holding the cyberbully liable, not to mention the school or the bully's parents, assumes that their identity is known. However, anonymity in cyberspace means that 41% of recipients[83] or victims[84] do not know.[85]

Civil actions

If the bully's identity is known, a child's age is no barrier to civil liability:

> *A child is personally liable for the consequences of his wrongful acts. That is certainly so if he was old enough to know that his conduct was wrongful – that is to say if, in the common phrase, he was old enough to know better.*[86]

As such, the recipient may have an action in the tort of assault, *Wilkinson v Downton*[87] or defamation.[88] In practice, it would not be desirable to bring a civil action against the bully, given their probable lack of funds to meet any damages award.[89] These actions have further limitations.

Take the example of assault. A phone call, text message or post on a website threatening that the recipient is going to be killed or bashed in the very near

---

principal brought actions in defamation and intentional infliction of emotional distress against J S. They brought an action in negligent supervision against his parents. On 2 November 2000, Allentown's *Morning Call* newspaper announced that the Supreme Court of Pennsylvania had decided the teacher's case in her favour. She was awarded $500,000 in damages. The damages were not awarded for defamation, but for invasion of privacy and, more importantly for present purposes, negligent supervision by his parents. See also Erb, above n 34, 278.

[83] I use "recipient" in the context of civil actions.

[84] I use "victim" in the context of criminal actions.

[85] Shariff and Hoff, above n 50, 82; Qing Li, 'Cyberbullying in Schools: Nature and Extent of Canadian Adolescents' Experience' (Paper presented at the Annual Meeting of the American Education Research Association (AERA), Montreal, April 2005) 1.

[86] *McHale v Watson* (1964) 111 CLR 384, 386-387 (Windeyer J).

[87] A claim that they have suffered harm in the form of a diagnosable psychiatric condition.

[88] Campbell, Butler and Kift, above n 21, 24; Butler, above n 21, 52; Kift, Campbell and Butler, above n 21, 81-83; Butler, Kift and Campbell, above n 21, 98-105.

[89] Kift, Campbell and Butler, above n 21, 81; Butler, Kift and Campbell, above n 21, 97.

future – perhaps during recess, lunch or after school – would satisfy the immediacy requirement.[90] However, if the likely infliction of the threat of violence is more remote, which is often the case in cyberbullying,[91] it may be difficult to argue that the bully has committed an assault.[92]

Similarly, if the recipient can show that they have suffered harm in the form of a diagnosable psychiatric condition, they may be able to establish a *Wilkinson* claim.[93] However, usually the recipient will only suffer harm, such as stress, anxiety or fear, which is insufficient.[94]

Although a post made on a social media, such as Facebook, will easily satisfy the element in a defamation action of publication to a third party,[95] cyberbullying may involve a private communication such as a text message between the bully and recipient, which would not satisfy this element.[96] The requirement that the matter complained of is defamatory may not be satisfied either, as statements, however abusive or insulting, may be true.[97]

Criminal actions

If a child is 10 years of age or older, they may be held criminally responsible.[98] The *Criminal Code Act 1995* (Cth) prohibits the misuse of a carriage service to make a threat, for a hoax or to menace, harass or cause offence. A carriage service is a telephone service (for example, Telstra) or

[90] Kift, Campbell and Butler, above n 21, 83; Butler, Kift and Campbell, above n 21, 99.
[91] Lipton, above n 51, 99.
[92] Kift, Campbell and Butler, above n 21, 83; Butler, Kift and Campbell, above n 21, 99.
[93] [1897] 2 QB 57; Kift, Campbell and Butler, above n 21, 83; Butler, Kift and Campbell, above n 21, 100.
[94] Kift, Campbell and Butler, above n 21, 83.
[95] Ibid 82; Eva English, 'Liability for bullying: Holding schools accountable' (2011) 19 *Tort Law Review* 41, 44; S Auerbach, 'Screening Out Cyberbullies: Remedies for Victims on the Internet Playground' (2009) 30 *Cardozo Law Review* 1641, 1667.
[96] English, above n 95, 44; Auerbach, above n 95, 1667.
[97] English, above n 95, 44; Auerbach, above n 95, 1667; Butler, Kift and Campbell, above n 21, 105; *Donoghue v Hayes* (1831) Exch 265, 266; *Entienne Pty Ltd v Festival City Broadcasters Pty Ltd* (2001) 79 SASR 19, 28-29.
[98] Campbell, Butler and Kift, above n 21, 24; Kift, Campbell and Butler, above n 21, 70; Butler, Kift and Campbell, above n 21, 88.

an ISP (for example, Telstra-Bigpond). Specifically, a bully commits an offence if they use a carriage service:

- to make a threat to kill, or cause serious harm to, the victim or another person and the bully intends the victim to fear that the threat will be carried out;[99] or
- to send a communication and the bully does so with the intention of inducing a false belief that an explosive, or a dangerous or harmful substance or thing, has been or will be left in any place;[100] or
- in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.[101]

None of the offences explicitly require repetition of the bullying behaviour. This is of particular relevance to the last offence. Whether communication is menacing, harassing or offensive is not dependent on the number of posts on social media. The Act recognises the tendency for one online video, for example, to go viral.

Anti-stalking legislation may also provide an effective remedy because:

- the breadth of potential stalking behaviour and the net of liability are wide;
- it is sufficient that the bully intends to induce in the victim an apprehension or fear of either physical or mental harm; and
- the immediacy element is irrelevant.[102]

However, the legislation cannot deal with stalking conduct via the Internet that occurs internationally.[103] This would be a barrier if the bully and others

[99] *Criminal Code Act 1995* (Cth) s 474.15.
[100] Ibid s 474.16.
[101] Ibid s 474.17.
[102] *Crimes Act 1900* (NSW) s 545B; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) ss 8, 13; Kift, Campbell and Butler, above n 21, 73; Butler, Kift and Campbell, above n 21, 92, 94.
[103] Kift, Campbell and Butler, above n 21, 75.

post mocking comments, images or videos about the victim, but they do not know the victim and are not in the same jurisdiction as the victim.

Risk management strategies to deal with cyberbullying

Returning to consider cyberbullying in schools, the question is, what steps ought the reasonable teacher take to minimise the risk of injury from cyberbullying materialising? Schools should ensure that they have in place both proactive and reactive risk management strategies to prevent and respond to cyberbullying. Some strategies, such as the implementation of a school's bullying policy, are both proactive and reactive because they set out how school leaders and teachers should prevent *and* respond to cyberbullying. Other strategies, such as the implementation of the eSmart Schools program, are purely preventative, whilst others, such as the implementation of a school's discipline policy, are purely responsive. I recommend that schools give serious consideration to the following:

Amend your bullying policy

All government schools in New South Wales must implement the Department of Education's policy dealing with the prevention and response to bullying of students.[104] The policy explicitly includes cyberbullying and

[104] NSW Department of Education, *Bullying of Students – Prevention and Response Policy* (22 June 2018) NSW Government, 2.2.1 <https://education.nsw.gov.au/policy-library/policies/bullying-of-students-prevention-and-response-policy>. All state and territory education departments have similar policies or guidelines and templates for developing such policies. For Victoria, see the Department of Education and Training's "Bullying Prevention Policy" and "Student Engagement and Inclusion Guidance". For Queensland, see the Department of Education's "Working Together: A tool kit for effective school based action against bullying". For South Australia, see the Department of Education's "Cyber-bullying, e-crime and protection of young people – information for families". For Western Australia, see the Department of Education's "Guidelines for preventing and managing bullying in schools". For Tasmania, see the Department of Education's "Secretary's Instructions No 3 for Unacceptable Behaviour of Students and Volunteers at, and Visitors to, State Schools or School Activities", "Social Media Policy" and "Social Media Guidelines". For the Northern Territory, see the Department of Education's "Mobile phones and electronic devices in the school environment" policy and guidelines and "Suitable Text and Media Resources guideline". For the Australia Capital Territory, see the Education Directorate's "Safe and Supportive Schools" policy and procedures.

addresses the issue of a school's duty of care beyond school premises and before and after school hours:

> *This policy applies to all student bullying behaviour, including online (cyber) bullying, and applies outside of school hours and off school premises where students have been involved and there is a clear and close connection to the school.*[105]

Likewise, non-government schools should ensure that they not only implement policies preventing and responding to bullying, but also ensure that those policies include cyberbullying and address the time and geographical limits of the school's duty of care.

Amend your acceptable use of ICT resources policy

The National Safe Schools Framework states that all Australian schools need "[a]greements for responsible use of technology by staff and students."[106]

The NSW Department of Education has an "Online Communication Services: acceptable usage for school students" policy.[107] The policy applies to all students at government schools "who access Internet and online communication services within the Department network and from any external location."[108] It explicitly targets those students who use the Department network from home or elsewhere to cyberbully. Under the policy, students who use the Internet and online communication services provided by the Department agree to abide by the conditions of acceptable usage.[109] This includes not sending or publishing offensive or abusive

---

[105] Ibid 2.2.2.
[106] Standing Council on School Education and Early Childhood, *National Safe Schools Framework* (2013) 6, 3.4, <https://studentwellbeinghub.edu.au/docs/default-source/nationalsafeschoolsframework-pdf.pdf?sfvrsn=0>.
[107] NSW Department of Education, *Online Communication Services: acceptable usage for school students* (17 July 2018) <https://education.nsw.gov.au/policy-library/policies/online-communication-services-acceptable-usage-for-school-students?refid=285859>.
[108] Ibid 2.2.1.
[109] Ibid 1.1.5.

comments or threatening, bullying or harassing another student.[110]

Again, non-government schools should ensure that they not only implement policies dealing with acceptable use of ICT resources, but also deal in those policies with the use of their network from students' homes and other external locations.

Train your staff

In relation to bullying generally, the National Safe Schools Framework[111] recommends training for all staff in:

1. understanding what is happening in the school, making use of appropriate information gathering methods and related discussion;
2. positive student management;
3. knowledge and skills relating to methods of addressing bullying and harassment;
4. identifying and dealing with prejudice and discrimination, for example, as they relate to gender, race, sexuality, disability and other factors; and
5. understanding the effects of bullying and harassment on children and young people.

Staff should also receive ongoing professional development about emerging changes in research and technology related to student safety and wellbeing.[112] This could include changes in technology related to cyberbullying.

[110] Ibid 4.1.1.
[111] Ministerial Council on Education, Employment, Training and Youth Affairs Taskforce on Student Learning and Support Services, *National Safe Schools Framework*, 7-8 <http://www.scseec.edu.au/site/DefaultSite/filesystem/documents/Reports%20and%20publications/Archive%20Publications/Safe%20School%20Env/National%20Safe%20Schools%20Framework%20-%202003.pdf> .
[112] Standing Council on School Education and Early Childhood, above n 106, 7, 4.2.

Educate and warn your parents

As the Court of Appeal in England has already noted,[113] parents have significant responsibilities in relation to bullying. Schools ought to bring this to the attention of parents, warning them of the dangers to their children of life in cyberspace and either helping the parents to know how to help their children or, at least, pointing the parents to other sources of help. Practical ways in which schools can do this are discussed below.

Educate and warn your students

There is much good material available to help schools to educate and warn their students. A starting point could be the information about the National Safe Schools Framework on the website of the Department of Education and Training.[114] Practical examples of how schools might do this are also discussed below.

Strengthen your pastoral care programs

Leah Bradford-Smart's teacher, Mrs Ashworth, was a great example for those aspiring to good pastoral care:

> *Leah was closely and affectionately monitored by Mrs Ashworth, who saw to it that any threats raised at home were never fulfilled, and unostentatiously contrived to give Leah the support and encouragement she needed to deal with the problems which confronted her at school. Without the dedication and experience of Mrs Ashworth, or a teacher like her, the problems at home might well have developed into bullying at school. As it was they did not.*[115]

[113] *Bradford-Smart v West Sussex County Council* [2002] EWCA Civ 7, [25].
[114] See Department of Education and Training, *Student Resilience and Wellbeing Resources – The National Safe Schools Framework* (31 May 2018) Australian Government <https://www.education.gov.au/student-resilience-and-wellbeing-resources>.
[115] *Bradford-Smart v West Sussex County Council* [2002] EWCA Civ 7, [25].

Implement cyberbullying prevention activities

One of the guiding principles in the National Safe Schools Framework is the implementation of programs and processes to nurture a safe and supportive school environment. Preventing cyberbullying, through the implementation of programs and processes, helps schools to create this environment. I consider below two related Australian programs – eSmart Schools and the eSmart Digital Licence – which have improved cyber safety, increased digital literacy and reduced cyberbullying. I also consider ReThink, a program that originated in the United States, which has been successful in combating cyberbullying in the United States and beyond.

Case study – eSmart Schools

The eSmart Schools program supports the creation of a cyber-safe environment and, in so doing, helps schools to meet their duty of care. It is an initiative of the Alannah and Madeline Foundation, which is aligned with the Australian curriculum and endorsed by the Office of the eSafety Commissioner. Your school may already be amongst the 2,200 Australian schools currently using eSmart.[116]

It is important that school leaders, teachers and the rest of the school community familiarise themselves with the world of cyberspace and ways of dealing with its downsides. eSmart Schools is one way of doing this. The online system provides schools with tools and resources to help equip school leaders, teachers and the rest of the school community with the skills and knowledge to manage cyberbullying and other cyber risks (for example, sexting) and foster smart, safe and responsible use of technology.

The content of the program covers six areas: effective school organisation; school plans, policies and procedures; a respectful and caring school

[116] Participating schools cover Government, Independent and Catholic sectors and include primary and secondary, as well as combined schools.

community; effective teacher practices; an eSmart curriculum; and partnership with parents and local communities.

The program is delivered in a two-stage process:

- Firstly, schools are prompted to review their current policies and practices to find technology, procedural and cyber safety gaps and, if need be, they are guided through the introduction of new policies and practices. It is helpful for schools to be reminded to keep their policies and practices up to date. However, in principle it is always a good idea for schools to seek legal advice when reviewing, and before introducing, policies and practices.
- Secondly, teachers are guided through a series of modules to improve their understanding of expected online behaviours and knowledge of how to manage cyberbullying and online incidents. Their progress is tracked and recorded. They can pass their understanding and knowledge onto their students and the parents.

Once complete, the school achieves eSmart status. Most schools take an average of 18 months to obtain this status. Clearly, this is not a quick fix solution. As the Foundation says, it is a long-term solution focused on "cultural-change" within and beyond schools.[117]

The program targets schools and teachers. Students and parents benefit by extension. The idea is that by embedding smart, safe and responsible use of technology across the curriculum, students will be educated about cyber safety, which should go some way to preventing cyberbullying.[118]

[117] Alannah & Madeline Foundation, *eSmart Schools* <https://www.amf.org.au/media/2445/esmart-schools-factsheet-2018.pdf >.
[118] For more information, see Alannah & Madeline Foundation, *eSmart Schools* (2018) <https://www.esmart.org.au/esmart-schools/>.

Case study – eSmart Digital Licence

A program that not only targets teachers, but parents and students, is the eSmart Digital Licence. Your school may already have some of the 200,000 students that have been registered for the eSmart Digital Licence.

It is an online challenge consisting of eight modules which use interactive quizzes and learning resources, such as videos and games, to evaluate students' digital literacy and cyber safety knowledge and teach them how to play, learn and socialise online in a smart, safe and responsible way. It can be purchased by teachers for students to complete at school and by parents for their children to complete at home.[119]

Teachers can track the progress of their students and they are given support and resources, such as open-ended lesson guides for each key learning area and these are linked to the Australian curriculum. Parents can access resources to learn the key elements of the digital environment to gain confidence and engage in a digital conversation with their children.[120]

Case study – ReThink

Whereas the Australian programs use education to prevent cyberbullying, the United States program, ReThink, uses technology to detect and prevent cyberbullying.

The ReThink technology can be customised to fit school devices and computers. Once installed, if a student tries to post an offensive message, the ReThink technology will detect the offensive language. An alert will appear giving the student a chance to reconsider before posting. The student can then decline to post the offensive message.[121] In this way, the program

[119] For teachers, it is $10.00 per student. For parents, it is $30.00 per child. eSmart Schools is available to all schools for $3,500.00 plus GST per school/campus.
[120] For more information, see Alannah & Madeline Foundation, *eSmart Digital Licence* <https://www.digitallicence.com.au/>.
[121] ReThink, *What is ReThink?* (2018) <http://www.rethinkwords.com/whatisrethink>.

aligns with restorative justice principles as it focuses on bringing about behavioural change for the cyberbully.

The statistics indicate that the program has been successful in doing this. When students are alerted to reconsider their decision, they change their minds 93% of the time.[122] Using ReThink, the overall willingness of a student to post an offensive message reduced from 71% to 4%.[123]

The program has experienced a great deal of success in the United States and beyond. In Michigan, 1.3 million students have been given access to the ReThink technology as part of the OK2SAY program.[124] Over 1,500 schools around the world have also had the technology installed.[125]

Responding to cyberbullying

The programs in Australia and the United States that I have discussed are proactive in that they are designed to prevent cyberbullying. Of course, it is possible that cyberbullying may still occur. If it does, schools should respond in accordance with their policies. This should include disciplining the cyberbully. However, schools should also be aware of social media services' complaints schemes and the complaints system established by the *Enhancing Online Safety Act 2015* (Cth).

Discipline

Cyberbullying is presumably prohibited in all schools. Therefore, any cyberbullying is a breach of school rules and may be subject to discipline. However, the appropriate discipline may vary depending on the situation. In some situations, the school may want to consider taking a restorative justice approach to attempt to reconcile the students. In other cases, the school may need to consider suspension or expulsion.

---

[122] Ibid.
[123] Ibid.
[124] ReThink, *ReThink For Schools* (2018) <http://www.rethinkwords.com/schools>.
[125] ReThink, *To stop online hate before the damage is done* (2018) <http://www.rethinkwords.com/>.

Schools should follow their discipline policies and, when appropriate, involve the students' parents. Often parents will not accept that their child is cyberbullying another student. In these situations the school may need to think through how it communicates with the parents to avoid potential conflict.

However, discipline is only one aspect of how a school should respond to cyberbullying. Schools need to take all reasonable precautions to prevent risks of harm to their students. It is unlikely that there will ever be a situation in which disciplining a cyberbully will be the only reasonable precaution that a school should take.[126]

Social media services' complaints schemes

School leaders and teachers may see or hear that seriously threatening, intimidating, harassing or humiliating material is being circulated on social media about one of their students. It could be brought to their attention by the cyberbullied student, by a friend of theirs or by the school's Internet monitoring software.

The school should respond in accordance with its bullying and discipline policies. The bullying policy will likely require school leaders and teachers to inform the student's parents that they have reason to believe that their child is being cyberbullied. The logical first step would be to ask the cyberbully to remove the offensive post, image or video from social media.

However, if the cyberbully refuses to remove the offensive post, image or video, school leaders and teachers should advise the affected student and their parents that social media services have complaints schemes under which requests can be made for the removal of cyberbullying material that breaches the service's terms of use.

---

[126] For more information, see Emil Ford Lawyers, *Education Law Articles – Discipline* <https://www.emilford.com.au/education-schools/education-law-notes/education-law-articles-discipline/>.

Note that most social media services' complaints schemes are set up so that the complaint must be made by the student themselves – not by their parents or teacher on their behalf. However, the teacher may wish to show the student and their parents how to make a complaint.[127]

Complaints to the eSafety Commissioner

Once a complaint has been made under Facebook's complaints scheme, or that of any other social media service, if the bullying post, image or video is not removed within 48 hours,[128] recourse can be had to the complaints system established by the *Enhancing Online Safety Act 2015* (Cth). Section 18 of the Act reads:

(1) If an Australian child has reason to believe that he or she was or is the target of cyber-bullying material that has been, or is being, provided on a particular social media service or relevant electronic service, the child may make a complaint to the Commissioner about the matter.
(2) If:

> *(a) a person (the responsible person) has reason to believe that cyber-bullying material targeted at an Australian child has been, or is being, provided on a particular social media service or relevant electronic service; and*
> *(b) either:*
>
> > *(i) the responsible person is a* ***parent*** *or guardian of the child; or*
> > *(ii) the child* ***has authorised the responsible person*** *to make a complaint about the matter;*

the responsible person may, on behalf of the child, make a complaint to the Commissioner about the matter.

---

[127] For more information, see Facebook, *Empower Educators* (2016), 5 <https://scontent.fsyd7-1.fna.fbcdn.net/v/t39.2365-6/14677812_818010928340505_8480908462098743296_n.pdf?_nc_cat=0&oh=f8464f72574c361fb939b40d912719bf&oe=5C3AE227> .
[128] *Enhancing Online Safety Act 2015* (Cth) ss 29(1)(c)(i), 35(1)(c)(i).

School leaders and teachers should ask the student and their parents about the progress of the complaint made under the social media service's complaints scheme. If the matter has not been resolved, they should inform the student that they may make a complaint to the Commissioner themselves and the parents they may make a complaint to the Commissioner on behalf of their child.

Although unlikely, it is possible that it may fall to the school to make a complaint to the Commissioner on the student's behalf. I draw school leaders and teachers' attention to the fact that, before they can do so, **the student must authorise them** to make the complaint. Whether the student has the capacity to authorise them is a question of fact. It will depend on the student's age and maturity. That said, it is a prerequisite for making a complaint to the Commissioner that a complaint has already been made under the relevant social media service's complaints scheme. As previously mentioned, these schemes are set up so that the student must make the complaint. If the student has the capacity to make a complaint to the social media service, it is likely that they also have the capacity to authorise a school leader or teacher to make a complaint to the Commissioner on their behalf.

Regardless of who makes the complaint to the Commissioner, it must be accompanied by evidence that the bullying post, image, video or the like was the subject of a previous complaint made under the relevant social media service's complaints scheme.[129] Evidence includes, but is not limited to, a receipt or complaint number, screen shot or statutory declaration.[130]

The Commissioner may investigate the complaint.[131] If the relevant social media service is "Tier 1", that is, airG, Roblox, Yubo, ASKfm, Snapchat,

[129] Ibid s 18(4)-(5).
[130] Ibid s 18(7)-(9).
[131] Ibid s 19(1).

Yahoo!7 Answers, Flickr, Twitter, Yahoo!7 Groups or musical.ly,[132] the Commissioner may **request** the service to remove the material within 48 hours.[133] If the relevant social media service is "Tier 2", that is, Facebook, Instagram, Google+ or Youtube,[134] the Commissioner may **require** the service to remove the material within 48 hours.[135] Non-compliance may result in civil penalties, enforceable undertakings and injunctions.[136]

Conclusion

If the 1800s adage "sticks and stones may break my bones but words will never hurt me" was ever representative of how individuals responded to bullying then, it no longer holds true in today's society. It is clear that words, together with images and videos, transmitted online may not only hurt, but can (and indeed have) led bullied children and teenagers to take their own lives.

This is the social and technological climate in which today's schools find themselves. It is clear that when students are at school, the school owes them a duty of care. However, it has also long been established that a school's duty of care does not cease upon the ringing of the final bell of the day or stop at the school gate. It extends beyond school premises and outside of school hours.

This makes a school's responsibility when it comes to protecting its students from cyberbullying all the more difficult. Unlike physical bullying (for example, punching), social bulling (for example, leaving people out) and verbal bullying (for example, name calling and put downs), which can be seen or heard by teachers, cyberbullying is silent and done with the touch of a keyboard or the tap of a screen. Nevertheless, it is possible that a school

---

[132] Office of the eSafety Commissioner, *Social media partners* Australian Government <https://esafety.gov.au/social-media-regulation/social-media-partners>.
[133] *Enhancing Online Safety Act 2015* (Cth) s 29(1)(g)-(h).
[134] Office of the eSafety Commissioner, above n 132.
[135] *Enhancing Online Safety Act 2015* (Cth) s 35(1)(f)-(g).
[136] Ibid ss 35(1), 36, 46-48.

will be liable for cyberbullying conducted via a school-hosted website accessed away from school premises outside of school hours using personal computers.

Since cyberbullying may fall within the ambit of a school's duty of care, and because the risk of cyberbullying is clearly foreseeable and more than insignificant, schools must consider what reasonable precautions they ought to take to minimise the risk of harm to students through cyberbullying. My plea is for all schools, as a starting point, to ensure that their bullying and discipline policies cover cyberbullying and their policies dealing with acceptable use of ICT resources cover the use of the school's network from students' homes and other external locations. Once the policies are up-to-date and in place, make sure they are followed!